CERTIFICATE OF AUTHENTICITY

OF DATA COPIED FROM AN ELECTRONIC DEVICE, STORAGE MEDIA

PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(14)

I, Josh Saltar, attest and certify, under penalty of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in the certification is true and correct.

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since October 2014. During my employment, I have received numerous forensic trainings with the Department of Defense, from my prior job with the U.S. Air Force at the National Air and Space Intelligence Center, the Department of Justice, as well as from private sector security digital forensics conferences. I have received multiple certifications in Windows, mobile, and memory forensics, as well as incident response and penetration testing, and am certified by the Department of Justice as a Digital Extraction Technician (DExT). As both a SA and DExT, I have received extensive training and experience in forensic imaging of electronic devices and mass storage media, including hard drives, mobile devices, removable flash storage media, and optical media. I have worked with multiple international law enforcement agencies around the world, focusing on cyber-terrorism and terrorist financing through computer intrusions. I have also assisted on various cases and violations, ranging from violent crimes against children and white collar to healthcare fraud, counterintelligence, and counterterrorism. Throughout those cases, I have worked with thousands of digital evidence items. I have made well over 500 forensic images of electronic devices and mass storage media during this time.

2. I am qualified to authenticate the extraction referenced in this paragraph because of my experience, training, and certifications.

Original Storage Media	Source	Date of Image
Apple iPhone 11 Pro Gray (614-581-5826)	1B10	July 21, 2020

3. The extraction described above is a forensically-sound image of the original cell phone.

4. The forensic image identified above was made using specialized forensic software named Cellebrite Physical Analyzer, version 7.35.1.15. In my training and experience, this forensic software creates an accurate and reliable forensic image of the cell phone at the time in which the forensic image is performed. I have regularly relied on this forensic process in the past.

5. Furthermore, I know that the forensic imaging process completed successfully because the forensic software identified that the device extraction completed successfully and without errors.

6. Based on my training, experience, and regular use of the forensic software described above, I know that the above-identified extraction is a forensically-sound image of the cell phone from evidence item 1B10.

I further state that this certification is intended to satisfy Rules 902(11) and 902(14) of the Federal Rules of Evidence.

Dec 30, 2022

Date

Josh Saltar
Special Agent
Federal Bureau of Investigation

CERTIFICATE OF AUTHENTICITY

OF DATA COPIED FROM AN ELECTRONIC DEVICE, STORAGE MEDIA

PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(14)

I, Brian Ledbetter, attest and certify, under penalty of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in the certification is true and correct.

1. I am employed by the Federal Bureau of Investigation (FBI), and my title is Digital Forensic Examiner (DFE). I have been in this position with the FBI since 2019. As a Digital Forensic Examiner, I have extensive training and experience in forensic imaging of electronic devices and mass storage media, including hard drives, mobile devices, removable flash storage media, and optical media. In my 3-year career as an FBI certified Forensic Examiner on the Computer Analysis Response Team (CART), I have worked over one hundred cases, involving hundreds of digital evidence items. I have made more than 200 forensic extractions of mobile devices during this time. In addition, I have successfully completed every annual proficiency test administered by the FBI's Digital Forensics Support Unit – Quality Assurance program that are required to maintain my FBI certification as a Digital Forensic Examiner.

2. I am qualified to authenticate the forensic extractions referenced in this paragraph because of my experience, training, and certifications.

Original Storage Media	Source	Date of Extraction
Apple iPhone 11, 256GB, Model: A2111, S/N: FK1ZF004N72Y	1B8	09/14/2020
Apple iPhone 11 Pro, 256GB, Model: A2160, S/N: F17ZT3E4N6XT	1B9	9/14/2020
Apple iPhone XR, 64GB, Model: A1984, S/N: G0N2215UKXKQ	1B13	07/21/2020
Apple iPhone 6, 64GB, Model: A1549, IMEI: 359296062145348	1B31	09/17/2020

3. The forensic extractions described above are true representations of the original mobile devices.

4. The forensic extractions of 1B8, 1B9, 1B13, and 1B31 were made using specialized forensic software. For items 1B8 and 1B9, GrayKey (OS: 1.6.7.9, App Bundle: 1.15.0) from GrayShift was used as the extraction tool. For item 1B31, GrayKey (OS: 1.6.7.11, App Bundle: 1.15.0) was used. For item 1B13, Physical Analyzer (v.7.33.0.30) from Cellebrite was used. These forensic tools were tested, validated, and approved for use by the FBI's Digital Forensics Support Unit. In my training and experience, these forensic software create an accurate and reliable forensic extraction of a mobile device at the time in which the forensic extraction was performed. I have regularly relied on these forensic processes in the past.

5. Furthermore, I know that the forensic extraction processes completed successfully because the forensic software generated a hash (i.e. digital fingerprint) of the extracted data and because the software expressly indicated that the extraction was successful.

6. Based on my training, experience, and regular use of the forensic software described above, I know that the above-identified forensic extractions are true duplicates of the original data that was extracted from evidence items 1B8, 1B9, 1B13, and 1B31.

I further state that this certification is intended to satisfy Rules 902(11) and 902(14) of the Federal Rules of Evidence.

12/29/22
Date

Brian Ledbetter
Digital Forensic Examiner
Federal Bureau of Investigation

CERTIFICATE OF AUTHENTICITY

OF DATA COPIED FROM AN ELECTRONIC DEVICE, STORAGE MEDIA

PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(14)

I, Jarrod Scott, attest and certify, under penalty of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in the certification is true and correct.

1. I am a Computer Forensic Specialist (CFS) with the Ohio Bureau of Criminal Investigation (BCI) and have been since June 2010. During my employment, I have received numerous forensic and computer trainings with the Ohio Peace Officer Training Academy (OPOTA), from my prior jobs with the Ohio Attorney General's Office working in Information Technology Services, as well as from private sector digital forensics and information technology organizations. I have received multiple certifications in Windows forensics, Mac forensics, mobile forensics, memory forensics, and incident response, as well as software programming and database. I am a Global Information Assurance Certification (GIAC) Certified Forensic Analyst (GCFA) and an OPOTA Evidence Recovery Specialist in a Digital Environment (ERSDE). As a CFS, I have received extensive training and experience in forensic imaging and data extractions of electronic devices and mass storage media, including hard drives, mobile devices, removable flash storage media, and optical media. I have worked with multiple law enforcement agencies around Ohio, assisting on various cases and felony violations. Throughout those cases, I have worked with thousands of digital evidence items.

2. I am qualified to authenticate the forensic data extractions referenced in this paragraph because of my experience, training, and certifications.

Original Storage Media	**Source**	**Date of Extraction**
Silver Apple iPhone 11 Pro Max	1B26 (BCI 001)	July 22,2020
Rose Gold Apple iPhone 8	1B27 (BCI 002)	July 22, 2020
Black Apple iPhone X	1B28 (BCI 003)	July 22, 2020

3. The data described above are forensically-sound extractions of the original cell phones.

4. The forensic extractions identified above were made using a specialized forensic tool named GrayKey. In my training and experience, this forensic tool creates an accurate and reliable forensic data extraction of the mobile device at the time in which the forensic data extraction is performed. I have regularly relied on this forensic process in the past.

5. Furthermore, I know that the forensic extraction process completed successfully because the forensic tool identified that the cell phone extractions completed successfully and without errors.

6. Based on my training, experience, and regular use of the forensic tool described above, I know that the above-identified data extractions are forensically sound duplicates of the original data contained on the cell phones referenced in this paragraph.

Original Storage Media	**Source**	**MD5 Hash**
Silver Apple iPhone 11 Pro Max	1B26	C5EDB3D60C339CCE90C38A0737D712B4
Rose Gold Apple iPhone 8	1B27	66396B2474948CF04CA0859198E9E346
Black Apple iPhone X	1B28	32FF7A26687FB4E5EAB0632697D5F2F7

I further state that this certification is intended to satisfy Rules 902(11) and 902(14) of the Federal Rules of Evidence.

01/05/2023
Date

Jarrod Scott
Computer Forensic Specialist
Ohio Bureau of Criminal Investigation